Vergaderjaar 2014–2015 Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1496

Vragen van het lid **Dijkhoff** (VVD) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie over *het bericht «rijksoverheid.nl was dupe van DDoS-aanval»* (ingezonden 13 februari 2015).

Antwoord van Minister **Blok** (Wonen en Rijksdienst) mede namens de Minister-President en de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie (ontvangen 9 maart 2015)

Vraag 1
Bent u bekend met het bericht «rijksoverheid.nl was dupe van DDoS-aanval»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het bericht dat rijksoverheid.nl en diverse andere websites plat werden gelegd door een DDoS-aanval? Is er meer bekend over de achtergrond van de aanval? Was er sprake van ingekochte «pesterij» om de sites plat te leggen of was dit een mogelijk rookgordijn om een hack of andere besmetting te verhullen?

Antwoord 2
Ja, dat bericht klopt. Eventuele motieven of achtergronden bij deze aanval zijn vooralsnog niet bekend. Het Ministerie van Algemene Zaken heeft aangifte gedaan.

Vraag 3
In hoeverre behoren de getroffen websites tot de vitale infrastructuur? Is het essentieel dat websites als rijksoverheid.nl ten alle tijden beschikbaar zijn voor publiek? Of is het platleggen van de websites «slechts» een hinderlijke overlast waar we eens in de zoveel tijd rekening mee moeten houden?

[1] Nos, 11 februari 2015, http://nos.nl/artikel/2018594-rijksoverheid-nl-was-dupe-van-ddos-aanval.html

ah-tk-20142015-1496
ISSN 0921 - 7398
’s-Gravenhage 2015

Antwoord 3
De getroffen websites maken geen deel uit van de vitale infrastructuur. Uiteraard zijn zij wel van groot belang voor het informeren van de burgers. Regelmatig vinden DDoS aanvallen plaats. In vrijwel alle gevallen worden deze met succes afgeslagen en blijft de aanval onopgemerkt voor het publiek. Heel 2014 had rijksoverheid.nl een uitval van 0%.
Daarnaast is het goed om te beseffen dat ondanks alle inspanningen er altijd een kans blijft op incidenten. Kwaadwillende personen vinden steeds weer mogelijkheden om nieuwe en aanvullende beveiligingsmaatregelen te doorbreken. Deze terugkerende aanvallen vragen om een continue inspanning en toenemende investeringen in tooling en maatregelen. Het gaat erom om tegen aanvaardbare kosten de risico's zo minimaal mogelijk te maken.

Vraag 4
In hoeverre zou het bieden van een back-up in geval van een cyberaanval soelaas kunnen bieden aan het publiek? Wat zouden de kosten zijn van zo'n back-up en acht de regering die kosten proportioneel?

Antwoord 4
Voor de getroffen sites bestaat een back-upvoorziening, die echter ook getroffen bleek. De leverancier zal een verbeterplan opstellen waarbij het Ministerie van Algemene Zaken en het NCSC nauw betrokken zijn. Onderdeel van dat plan zal zijn te regelen, dat deze back-up voorziening bij een DDoS aanval wel kan worden ingeschakeld.
Zie ook het antwoord op vraag 3.

Vraag 5
Binnen hoeveel tijd kon de overheid de burger informeren over de problemen op de websites en zijn hiervoor alternatieve kanalen beschikbaar?

Antwoord 5
De rijksoverheid heeft per direct de telefonische (1400) en e-mail beantwoording van de dienst voor publieksvoorlichting «Informatie rijksoverheid» ingezet om burgers te informeren over de storing. Daarnaast is ook het Twitterkanaal «Informatie rijksoverheid» gebruikt om de volgers te informeren.
Na het oplossen van de storing zijn alle vragen die bij het loket zijn binnengekomen alsnog per mail of telefoon beantwoord.